МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РЕСПУБЛИКИ КАЗАХСТАН

КАЗАХСКИЙ АГРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ САКЕНА СЕЙФУЛЛИНА

Обнаружение аномального трафика в IOT

Подготовил: Нургалиев Толеген

Научный руководитель: PhD, ассоц. проф. Жукабаева Т.К.

Цель: Исследование и анализ аномального трафика в IoT.

Задачи:

- Исследование существующих методов по анализу трафика Интернета вещей.
  - Исследование систем обнаружения вторжений на основе аномалий.
  - Выявление эффективных способов по обеспечению информационной безопасности
- Выявление возможных НСД

  Обнаружение аномалий на прикладном уровне

  Обнаружение аномалий в маршрутном и транспортном уровнях

Задачи и способности Интернета Вещей:

Обеспечения комфорта человеку

- Автоматизация процесса работы;
- Мониторинг человеческого здоровья

Локализация объекта: обнаружение наличия объектов на изображении и указание их местоположение с помощью ограничительной рамки.

- Умные и безопасные дома ;
- Организация дорожного движения.

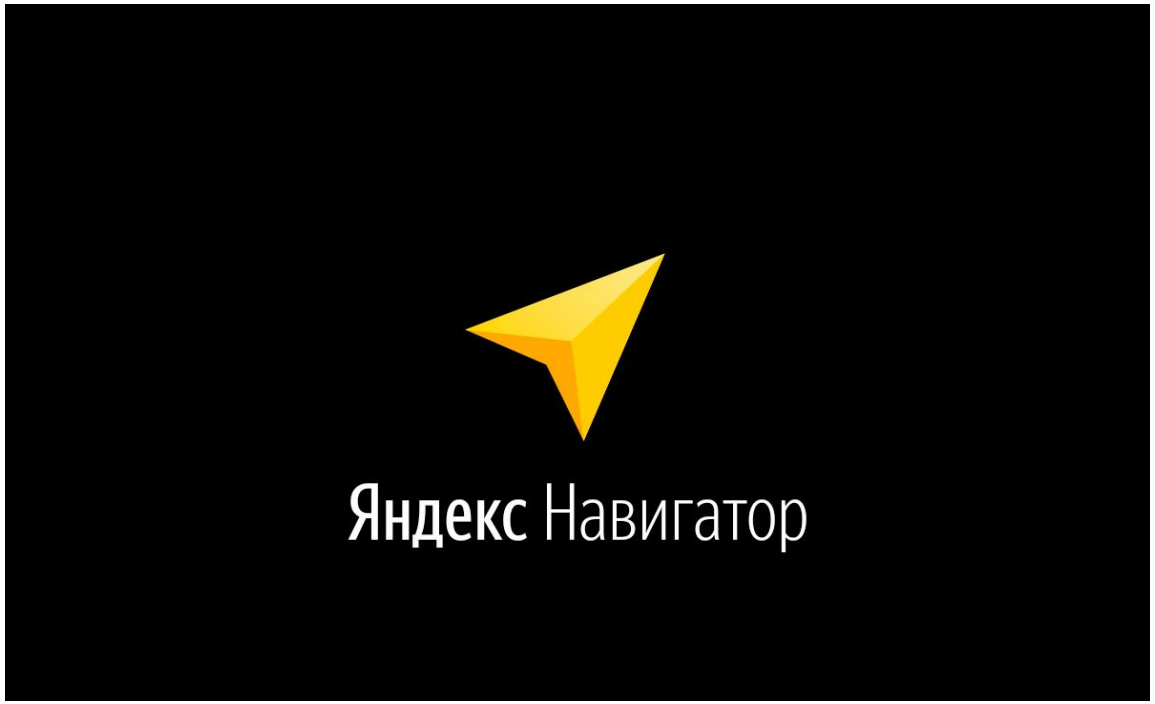
Обнаружение объектов: определение наличия у человека

Диспетчеризация и автоматизация съема показаний с приборов учета;

Существующие примеры применения Интернета вещей

Яндекс. Навигатор

Известная в России и в странах ближнего зарубежья система, есть не что иное, как использование IoT в управлении транспортом. Принцип действия следующий — гаджеты (планшеты, смартфоны) передают в компанию Яндекс направление движения автомобиля, координаты и скорость перемещения.



Вся информация анализируется на сервере и в обработанном виде передается на смартфон водителю, показывая заторы и пути их объезда.

То есть, обмен данными между сервером, приложениями и смартфонами происходит без участия человека и представляет собой пример использования интернет вещей.

Существующие примеры применения Интернета вещей

2. Умный дом

Китайская компания Xiaomi выпускает ряд устройств для умных домов. Это и смарт-электрика (розетки, выключатели, удлинители), и беспроводные контроллеры для управления другими гаджетами, и всевозможные датчики — движения, протечки воды, открывания дверей и окон, температуры, влажности и давления. Для большинства девайсов можно настроить сценарии поведения. К примеру, кнопка Xiaomi Smart Wireless Switch предлагает задать разные действия при одиночном щелчке, двойном или долгом нажатии, а Xiaomi Mi Magic Cube Controller, выполненный в виде кубика, можно повернуть, встряхнуть, постучать или сдвинуть — в зависимости от действия он умеет выполнять шесть команд, которые можно запрограммировать самостоятельно. Кнопка дверного звонка пришлет вам на смартфон сообщение, если кто-то придет к вам в ваше отсутствие, а при наличии камеры — еще и покажет фотографию гостя.

Существующие примеры применения распознавания объектов

2. Одно из подразделений компании General Electric, GE Renewable Energy, сумело снизить расходы на техническое обслуживание на 10 %, а расходы на внеплановый ремонт — на 20 %, внедрив систему мониторинга данных на своем полевом оборудовании. Филиал занимается выработкой энергии из возобновляемых источников и производит ветрогенераторы, электростанции на солнечной энергии, гидроэлектростанции. Специальные датчики в непрерывном режиме контролируют работу этого оборудования, передавая данные телеметрии в единый центр. При малейших отклонениях в работе специалисты GE готовы оперативно выполнить профилактические работы или срочный ремонт, предотвращая поломку и экономя средства на восстановление техники. Та же телеметрия позволяет предсказывать будущие объемы выработки энергии и планировать, как эффективнее использовать генераторы. Все это снижает эксплуатационные расходы и минимизирует финансовые потери компании.

Датчики температуры, давления, влажности — такие же, как в умных домах — могут использоваться и на предприятиях или складах, где эти показатели важны для технологического процесса или условий хранения. Автоматический климат-контроль поможет предотвратить появление брака и порчу готовой продукции. Электронике можно доверить и отслеживание сроков годности продуктов и товаров на складах. Системы управления могут отключать освещение после того, как последний сотрудник покидает рабочее место, включать охранную сигнализацию и отдавать команду на запуск робота-пылесоса.

Системы физической и кибербезопасности уже сегодня активно используют интернет. Камеры с датчиками движения автоматически включаются, когда в их поле зрения попадают перемещающиеся объекты, и отправляют видеозапись на серверы. Отчеты о событиях и подозрительной активности могут быть моментально направлены на email или смартфоны

Существующие примеры применения IoT

3 Tesla.

Обнаружение аномалий в инфраструктуре Интернета вещей (IoT) вызывает растущую озабоченность в области IT. С расширением использования инфраструктуры Интернета вещей в каждом обласьт человека соразмерно возрастают угрозы и атаки в этих инфраструктурах. Отказ в обслуживании, проверка типа данных, вредоносный контроль, вредоносная операция, сканирование, шпионаж и неправильная установка - это такие атаки и аномалии, которые могут вызвать сбой системы IoT. В этой статье сравниваются характеристики нескольких моделей машинного обучения для точного прогнозирования атак и аномалий в системах Интернета вещей. Здесь использовались алгоритмы машинного обучения (ML): логистическая регрессия (LR), машина опорных векторов (SVM), дерево решений (DT), случайный лес (RF) и искусственная нейронная сеть (ANN). Метрики оценки, используемые при сравнении производительности: точность, точность, отзывчивость, показатель f1 и площадь под кривой рабочих характеристик приемника. Система достигла 99,4% точности теста для дерева решений, случайного леса и ИНС.

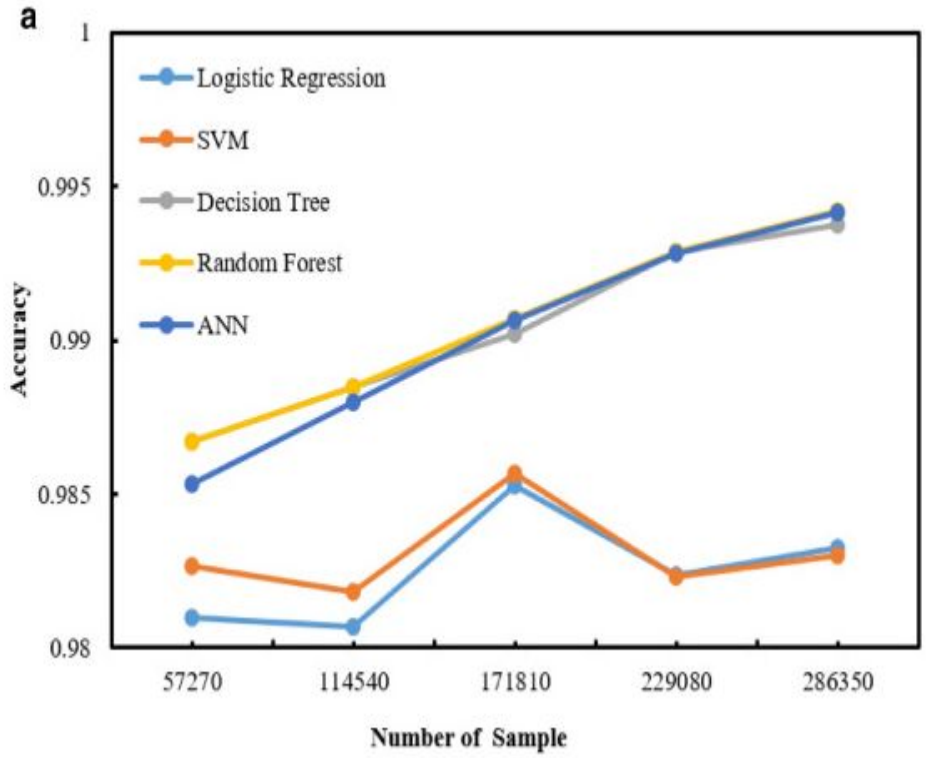
Набор данных с открытым исходным кодом был собран из kaggle , предоставленного Pahl et al(https://github.com/Shauqi/Attack-and-Anomaly-Detection-in-IoT-Sensors-in-IoT-Sites-Using-Machine-Learning-Approaches).

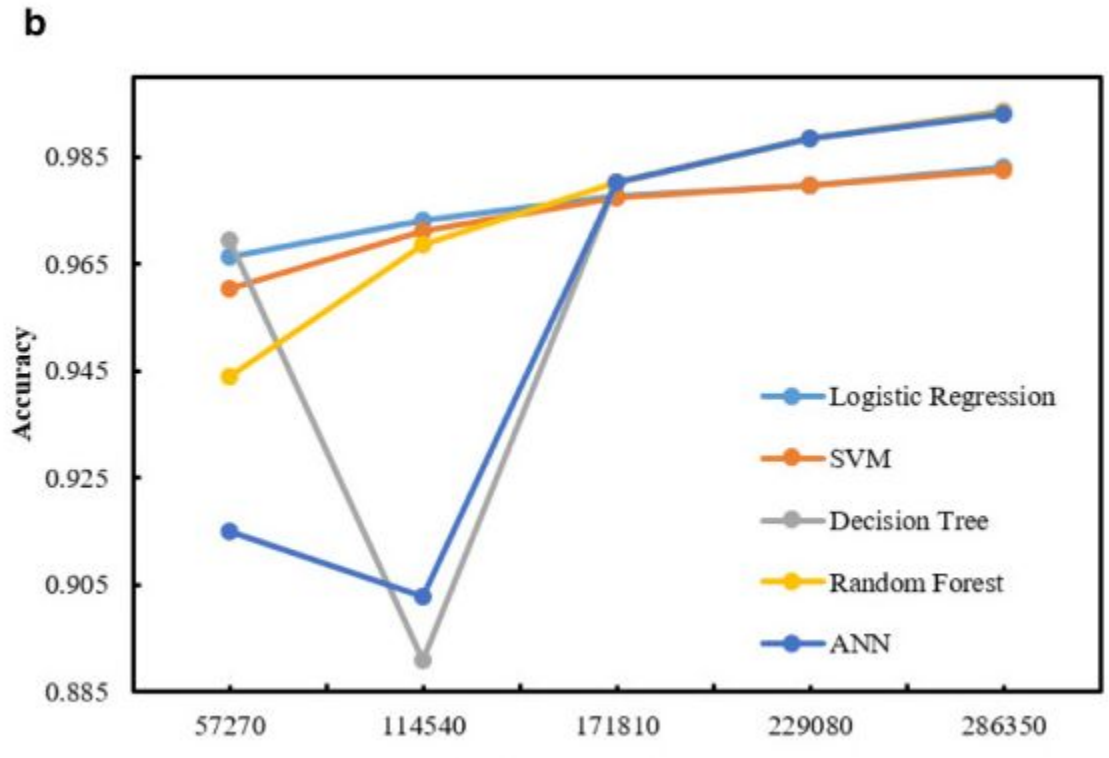
Attacks	Frequency Count	% of Total Data	% of Anomalous Data
Denial of Service	5780	01.61%	57.70%
Data Type Probing	342	00.09%	03.41%
Malicious Control	889	00.24%	08.87%
Malicious Operation	805	00.22%	08.03%
Scan	1547	00.43%	15.44%
Spying	532	00.14%	05.31%
Wrong Setup	122	00.03%	01.21%

алгоритмов глубокого обучения. Мы можем обучить модель ИНС, используя необработанные данные. По сравнению с другими классификаторами он имеет большое количество параметров для настройки, что делает его сложной структурой.

Анализ результатов

В подразделе «Анализ данных» было описано, что к набору данных было применено несколько методов машинного обучения. Пятикратная перекрестная проверка была проведена на наборе данных с использованием каждого из этих методов. . Из перекрестной проверки можно сделать вывод, что RF и ANN показали наилучшие результаты как в плане обучения, так и в плане точности тестирования.





Оценка		Классификаторы		
Метрики		LR	SVM	DT
Обучение	Точность	0,983	0,982	0,994
	СТАНДАРТНЫЙ (+/-)	0,0012	0,0015	0,00081
	Точность	0,98	0,98	0,99
	Отзывать	0,98	0,98	0,99
Тестирование	Точность	0,983	0,982	0,994
	СТАНДАРТНЫЙ (+/-)	0,0055	0,0064	0,016
	Точность	0,98	0,98	0,99
	Отзывать	0,98	0,98	0,99

Публикация
23 декабря 2020 года

ТЕМА: Обнаружение аномального трафика в IOT

Международная научная онлайн конференция
«ИННОВАЦИОННОЕ РАЗВИТИЕ ОБРАЗОВАНИЯ, НАУКОЕМКИХ ПРОИЗВОДСТВ И АЛЬТЕРНАТИВНЫЕ ИСТОЧНИКИ ЭНЕРГИИ»
Казахский национальный женский педагогический университет